UNCLASSIFIED

NMCI Deployables Operational Assessment (OA)

Test Director's Summary
15 April 2003

UNCLASSIFIED

Purpose

To evaluate the basic deployment process and capabilities provided by NMCI, and…

…to assess the system operational effectiveness, suitability, and survivability in an operational environment.

Test Participants

The DOA was comprised of three groups of participants:

- **Test Team.**
  - Test Director (LtCol Brian Mace, MFP)
  - Assistant Test Director (Maj Ed Taylor, 3-FSSG)
  - MCOTEA Test Team (Ed Spinella, Chuck Mock, Cathy Cabrera, and Andy Archetti)
  - MITNOC (GySgt Mark Casas) and MCTSSA (Bill Noble).

- **Data Collection Team.**
  - Data Collection Chief (1st Lt Criston Cox, 7th Comm Bn)
  - 5 Data Collectors (3rd Marines, CSSG-3, and MAG-24).

- **Test Subjects.**
  - 30 computer users (3rd Marines, CSSG-3, and MAG-24)
  - 2 Unit IT Reps (SSgt Rodriquez - CSSG-3 / Sgt Ponder - MAG-24)

Assessment Phases

- **Phase I** UITR/User/Data Collector Training 10 – 21 Feb
- **Phase II** Data Collection Pilot 24 – 26 Feb
- **Phase III** Pre-Deployment Garrison Ops 27 Feb – 3 Mar
- **Phase IV** Deployed Operations 5 – 12 Mar
- **Phase V** Post-Deployment Garrison Ops 17 – 21 Mar

Pre-Test Training

In order to familiarize the test participants with the nuances of the NMCI computers, processes, and procedures, the following training was conducted:

- Marine Corps Tactical Systems Support Activity (MCTSSA) Training.
  - Unit IT Rep (UITR) training for the 3 UITRs assigned to the DOA.
  - Excellent training, but not enough time built into the schedule.

- Information Strike Force User Familiarization Training.
  - Standard NMCI Rollout training.
  - 90 minute slide presentation on the basic operating procedures (password procedures, Outlook access, email procedures, Internet Explorer, ISF homepage contents, etc).
  - 30 minute one on one familiarization session at the user's laptop.
  - Useful training, but needs to emphasize differences. (Too generic).

- MCOTEA Data Collection Training.
  - Thorough training session for the Data Collection Chief and 5 Data Collectors.

Data Collection Pilot

- **Following the Training Phase, a Data Collection Pilot (Phase II) was conducted.**

- **The pilot served a dual purpose:**

  - Provided Test Subjects an opportunity for a dry run on the more complex tasks to be expected in the actual assessment.

  - Provided Data Collectors with an opportunity to smooth out their data collection procedures.

Record Test

- **The actual record test was comprised of three phases (Phases III, IV, & V) and was conducted at two separate sites.**

- **Phase III and V (Pre and Post Deployment Garrison Ops):**

  - CAS Trainer at Kaneohe Bay, Hawaii
  - 32 NMCI NIPRNET drops
  - SIPRNET RAS (CAS Trainer) / SIPRNET LAN (K-Bay server farm)

- **Phase IV (Deployed Operations:**

  - Pohakaloa Training Area (PTA) concurrent with the Hawaii CAX.
  - 3rd Marines TDN (PTA Base Camp).
  - MRC-142 (AN/MRC-142 Multichannel Radio Terminal Set) UHF shot.
  - CSSG-3 NIPRNET / SIPRNET TDN at forward deployed site.

Pre-Deployed Garrison Ops

- Verify currency of Norton Anti-Virus
- Verify ability to Migrate Data using internal and external media
- Verify accuracy of Gold Disk Media & Documentation
- Ensure Pack-up Kit (PUK) is received and contents are complete
- Save and Verify content in shared folders
- Obtain Global Address List from ISF (.csv files)
- Verify ability to execute Deployment [Ability to execute the Deployable App (DA 2.1)]
- Verify Email Redirection inactive prior to deployment

Deployed Operations

- Verify availability of Remote Access Service (RAS) Reachback
- Verify ability to upload and use Global Address List file
- Verify existence of sufficient Helpdesk troubleshooting support.
- Assess availability and usefulness of deployed seat rebuild tools.
- Verify receipt/adequacy of deployed user ID importation file.
- Verify Email redirection capability & failure notifications.
- Verify ability to upload migrated data to deployed environment.
- Verify Norton Anti-virus update capability during deployments.

Deployed Operations ..cont'd

- Assess de-activation of ISF Enterprise Management Software.
- Assess Outlook Web Access capability.
- Assess defective equipment reporting/return procedures.
- Assess ability to deactivate Email Redirection.
- Verify ability to enable DHCP capability prior to return.
- Verify completeness of "end item" spares returns.

Post-Deployed Garrison Ops

- Verify Email Redirection de-activated
- Verify removal of deployed users from NMCI GAL
- Verify existence of Automated Compliance/IA Scan upon return.
- Verify ability to migrate data back to NMCI environment.
- Verify integrity of Shared Folder Data (pre-deployed data store)
- Verify the ability to execute the Deployable App (DA 2.1)
- Assess return process for Gold Disk application media to ISF
- Assess adequacy of spares return process

Test Limitations

- **Garrison SIPRNET LAN - Only at Server Farm**
- **MITNOC / ISF GAL Process – Not yet established**

Test Director Observations

- **Inadequacy of Pack Up Kit (PUK):**
  - Delivered 6 days prior to the movement.
  - Documentation in support of the included media was outdated and did not support the model of computers issued (docs for Dell 610s vice Dell 640s).
  - Documentation riddled with corrections and page deletions.
  - Problems caused by PUK not fully realized until well into the Deployed Phase.
  - One spare laptop to support the 34 deploying computers (RO had no way to verify whether this was sufficient)
  - **Spare consumed within 72 hours, 2nd failure occurred late in the deployment (5.8% defect rate)**
  - Initially, PUK only supported the NIPRNET computers until requested. While the spares are generic, allowing configuration for either NIPRNET or SIPRNET, the media to support SIPRNET rebuilds (SIPRNET Gold Disk) was not included. The RO contacted ISF for resolution and the SIPRNET media was received the day prior to movement.

Bottom Line: Poor attention to detail.

Test Director Observations

- **Remote Access Service (RAS) Reachback:**
  - Most labor-intensive series of test events.

  Note: While RAS does provide a reachback capability, it is much more conducive to a garrison TAD environment than a tactical environment.
  - Problems encountered tied to physical infrastructure limitations.
  - **Incompatible with TA-1042 field phones.**
  - Connection speeds ranged from 14.4 to 28.8 Kbps (Lower connection speeds caused timeout issues during Internet Explorer website access)
  - Conducted entirely from base camp.
  - Connection Tasks:
    - Access and use Outlook email and directory functions
    - Access the internet through Internet Explorer
    - Access their shared folders
    - Connect to Outlook Web Access (OWA).
  - Initial Users: 4 hours; Average: 2 hours. UITRs present the entire time.
  - Repeated for SIPRNET.

Bottom Line: Unlikely to be used in a tactical environment.

Test Director Observations

- **Rebuild Gold Disk Inconsistencies:**
  - Computers = Alcatel VPN software / Rebuild Disk = TimeStep VPN software.
    - Problem for ALL system rebuilds.
    - No guiding documentation, further complicating RAS reachback.
  - No Norton Anti-virus Software on Rebuild Disk
    - Unhardened Rebuilds.
  - Computers = DA 2.1 / Rebuild Disk = DA 2.0.
    - Problem for ALL system rebuilds.
  - Computers = Current PAL application / Rebuild Disk = 2 versions older.
    - Disabled RAS capability for all rebuilt systems.

Bottom Line: Poor attention to detail.

Recommendation: Pre-Deployment Electronic Inventory

Test Director Observations

- **TA-1042 Tactical Field Phones.**
  - Incompatible with RAS operations.
  - Incompatible with NMCI automated helpdesk phone system.
    - Capable of making the initial helpdesk call.
    - Unable to progress through the automated selections (Not touch-tone capable)
    - ISF helpdesk system does not allow the user to “stay on the line for the next available operator.”

Recommendation: Modify automated helpdesk selections.

Test Director Observations

- **Growing Password/User ID /PKI Cert Requirements: (Provided for Info only)**
  - Current MCEN/TDN structure
    - Garrison & Deployed.
      - NIPRNET Domain User ID (example: smithja)
      - SIPRNET Domain User ID (example: smithja)
      - NIPRNET Domain Password
      - SIPRNET Domain Password
      - PKI Cert Password
  - After transition to NMCI, users must maintain the following:
    - Garrison (NMCI).
      - NIPRNET Domain User ID (example: "John.Smith")
      - SIPRNET Domain User ID (example: "John.Smith")
      - NIPRNET Domain Password
      - SIPRNET Domain Password
      - PKI Cert Password
      - Palladium Classified Modem Password
    - Deployed (TDN)
      - NIPRNET Domain User ID (example: smithja)
      - SIPRNET Domain User ID (example: smithja)
      - NIPRNET Domain Password
      - SIPRNET Domain Password
      - PKI Cert Password
      - Palladium Classified Modem Password

Test Director Observations

- **Public Keyed Infrastructure (PKI) Implementation.**
  - Additional layer of responsibility on the user.
  - Extraction prior to rebuilds
  - Trusted Agents

- Reference Materials and Training.
  - Marines learn by doing, not by reading.
  - “Fire Hose” Training is ineffective. Many sections of documentation were not covered.
  - **Recommend Immersion Training for UITRs.**

Test Director Observations

- **Deployable Application Backup.**
  - Obscure note in Deploy Process requires backup of the DA application at time of “Deploy”.
  - UITR was unable to reset the computer to the “Deployed” state. (Computer => “No Status”; Active Directory => “Deployed”).
  - The options for resolving this issue are:
    - Reload and Re-Deploy. Reload the DA 2.1, deploy the system, and return (“re-deploy”) the computer. The UITR could not accomplish this since DA 2.1 was not loaded on the Rebuild Gold Disk (See Section 9, “Gold Disk Inconsistencies”), only DA 2.0 was loaded, or
    - Helpdesk Assistance. Contact the Helpdesk to have the Active Directory flag reset to “Returned.” The UITR must then deploy and return (“re-deploy”) the system in order for the Administrative Rights to pass from the UITR back to ISF (Executing the “Deploy” function of DA 2.1 terminates all Enterprise Management Software and transfers Admin rights to the UITRs. Executing “Return” or “Re-Deploy” reverses the process.). During the DOA, option 2 was executed to resolve the issue.

Test Director Observations

- **Re-integration Issues._**
  - Software Compliance Scan appeared inactive.
  - Method: Application install date comparison (Before or after deployment).
  - Missing Norton Anti-Virus, Incorrect PAL version, Sniffer (all were allowed in).
  - No resolution through Nightly Connect.

- **Environmental Issues.**
  - Dust Intrusion (Keyboard / Floppy Disks)

- **Pre-Deployment Cutover and Computer Deficiencies.**
  - Problems accessing Outlook Public folders (4 laptops)
  - ISF Rebuilds: 1 repaired, 3 unresolved
  - Root Cause never identified.

Test Director Observations

- **NetBIOS (NB) Password Issues.**
  - NB password required for rebuilds (Boot Sequence/Media)
  - Enterprise NB password NOT desired by USMC.
  - Alternative: Manufacturer provided system specific PW (PW clearing PW).
  - Workaround: DOA specific password (4 ISF rebuilds allowed testing of Dell PW).

- **Customer Technical Representative (CTR) Engagement.**
  - Not recognized by ISF.

- **Helpdesk Training & Consistency.**
  - Unfamiliar with Deployed Operations
  - Incomplete troubleshooting/data collection on initial call (Spare Replenishment, etc.)
  - Complications on simple requests (Password Reset, Etc.)

Test Director Observations

- **Internet Explorer / Outlook Reconfiguration.**
  - Required after rejoining any network external to NMCI.
  - Labor intensive task for UITRs (Beyond the skill level of majority of users).

- **PUK Replenishment.**
  - Spare consumed within 72 hours.
  - Initial Helpdesk delay, followed by Dell onsite repair.

- **Blue Screens on Initial Attempt to Deploy.**
  - Occurred on 9 systems during initial “Deploy” attempt.
  - Error indicated “initiation of physical memory dump”
  - Resolved through reboot with no apparent data loss. Root Cause never identified.

Test Director Observations

- **Email & Public Folder Redirection.**
  - NIPRNET
    - Email: Successful via individual (web redirection tool, NMCI website) and group (Helpdesk) methods.
    - Outlook Public Folder: Successful via helpdesk request.
  - SIPRNET
    - Email: Initial helpdesk confusion stating "case by case decision, 90% disapproved." Eventually successful.
    - Outlook Public Folder: Denied by helpdesk as unauthorized.

- **IAVA Updates.**
  - MARFORINO released an IAVA (2003-A-0004) for Microsoft Internet Explorer.
  - MITNOC ("Can patch be installed without incurring MAC)=> Helpdesk => ISF IA Branch => West Coast ISSM: "First ever IAVA request"
  - Direction: Delay patch install until tested by ISF Lab
  - Resolution obtained after completion of OA (14 days of exposure).
  - Proposed Process: Release => ISF evaluation => MARFORINO for dissemination.

Legacy Applications Ops

- **DOA Intent: Test the NMCI Deployables Process.**
- **For added realism: Test Team identified four Legacy Applications that were believed to be ready for installation on the deployable laptops.**
- **Application Selection:**
  - Readiness for OA
  - Usefulness in normal daily routines.
  - Believed to require little or no interface with any external MCEN servers or databases.
- **Apps certified just prior to the DOA; insufficient time to load ISF NOC servers.**
  - Test Team made the call to allow ISF to load the LAs locally during K-Bay staging.

Legacy Applications Ops
cont'd

- **3270 Host on Demand.**
  - Relies on Terminal Emulation (TE) software for connectivity to a mainframe computer (not known at time of application selection).
  - ISF utilizes "Reflections for IBM (ver. 8.0.5)" as their TE software.
    - This TE software is configured to connect through an unsecured port. Under the USMC design, secure port 9023 is utilized. ISF policy does not allow use of this secure port. Based on the sensitive data (SSNs, etc.) transferred by 3270, the MITNOC recommendation was to avoid using the 3270 application in an unsecured configuration.
  - Test Director made the decision not to use it in garrison.
  - Deployed use of 3270 would be conducted the same as it is today between the TDN and MCEN.

Legacy Applications Ops
cont'd

- **Joint Message Processing System (JMPS).**
  - This application was installed on the systems and is used in drafting of Naval Messages. The Test Director evaluated the application and found it to be useable.

- **Asset Tracking Logistics and Supply System (ATLASS).**
  - Initial ISF load unusable (ISF provided diskette, located in the PUK, appeared corrupt)
  - Local copy offered to ISF.
  - Test Team made the call to allow installation by ISF. Installed app worked fine.

- **Unit Diary Marine Corps Integrated Personnel System (UDMIPS).**
  - Requires updates from a MCEN database.
    - During short-term deployments, these servers are NOT taken to the field. UDMIPS users transfer updates via email to accomplish their duties. Since the MCEN database was not visible to the NMCI computers, the users treated the entire DOA as a deployment, sending and receiving UDMIPS updates via email and working entirely off of the client.
  - The USMC Community of Interest (COI) is expected to resolve these connectivity issues.

Lessons Learned

- **Key Personnel Tasking.**
  - Excessive burden (UITRs)

- **Deployed Site/Realism.**
  - K-Bay / Pohakaloa Training Area (PTA)
  - Benefits of HCAX overlay / Realism
    - TA-1042 Field Phone Incompatibility
    - Environmental Issues
    - Remote Site PUK Replenishment / Onsite Repairs

- **Lack of clarity in overall NMCI Concept of Employment.**
  - USMC Community of Interest (COI).
  - Training of UITRs and NMCI Users.
  - Perpetually Deployed Units.
  - Global Address List (GAL) Solution.
  - Installation and Verification of Local Legacy Application.

Summary

- **Majority of concerns were attributable to “Process” vice “Capabilities.”**
  - Pack Up Kit deficiencies were completely avoidable, however, the lack of attention here created a significant and unnecessary burden on the deploying unit.
  - UITRs Training is critical to ease burden of disconnecting from NMCI, joining a deployed Tactical Data Network, negotiating tactical reconfigurations, and returning to the NMCI enclave smoothly (Possible solution: NMCI & Deployed Profiles)

Questions

Backup Slides

MAG-TA Concept

- Proposal: Allow Marine Aviation to exist on the peripheral of NMCI in order to preserve the rapid deployment capability of the MAG / MALS units.

- Currently pending approval by HQMC Aviation

MAG-TA Concept

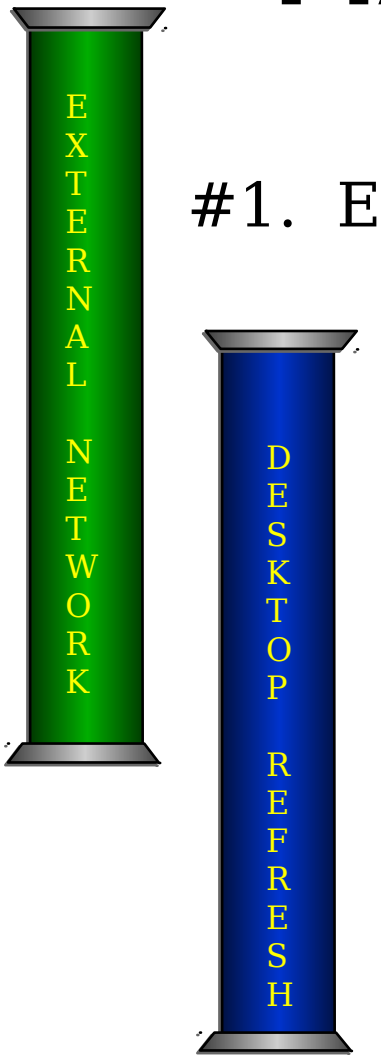
PRO

1. MAG/MALS' homogeneous configuration – supports tactical readiness posture
2. USMC network management and operation preserves tactical network skills
3. Enables connection of non NMCI Seats (UNIX based tactical AISs)
4. EDS loads legacy applications and connects to legacy network
5. Provides help desk support for the refreshed hardware
6. Desktop/laptop still refreshed in accordance with SLAs
7. Provides migration path to NMCI, if refinement in NMCI deployment process
8. Receives NMCI Gold Disk

CON

1. USMC management of an additional non-NMCI network component
2. USMC IT personnel continue to support MALS Aviation IS Department

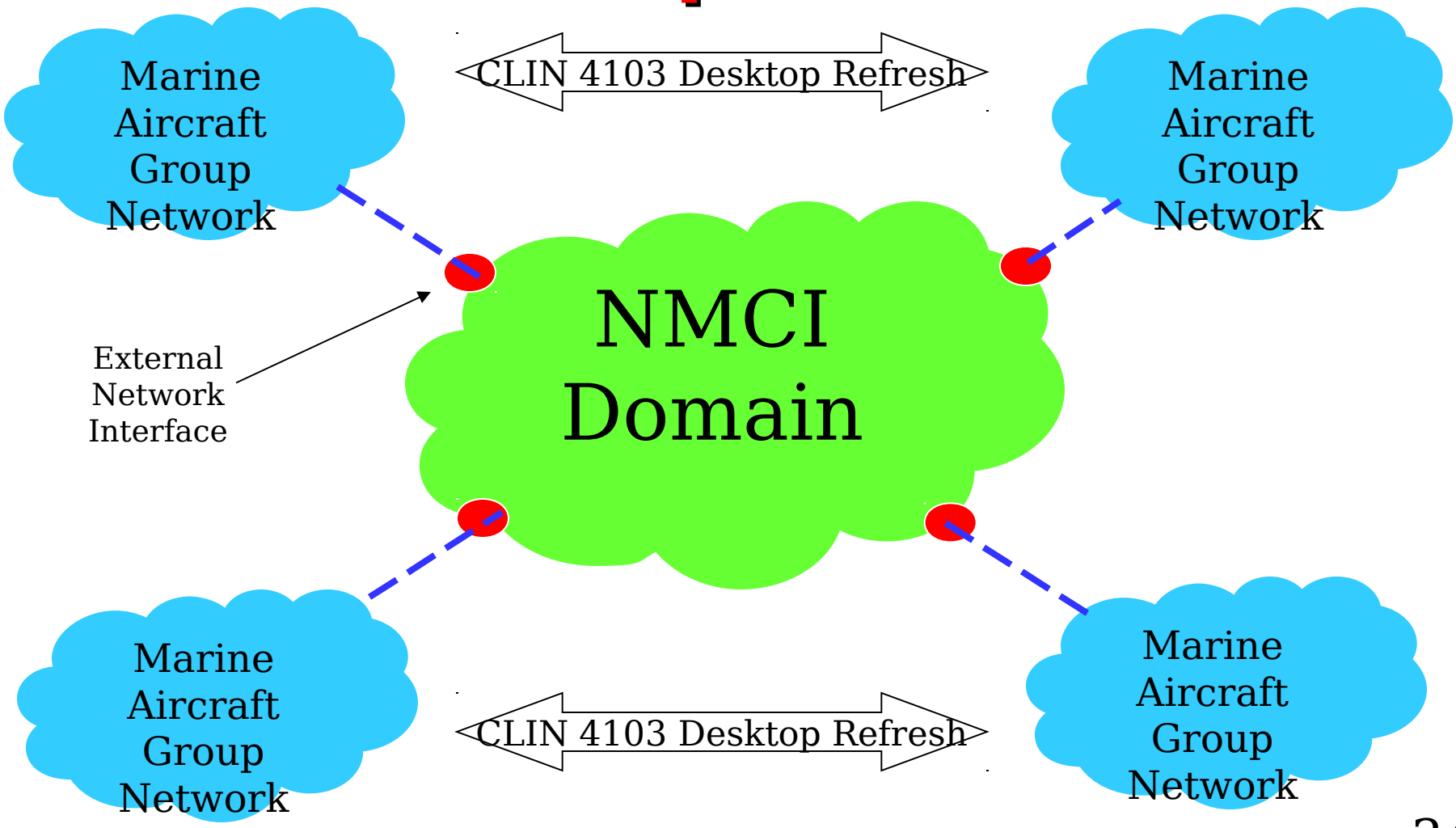
Two Key Pillars of MAG-TA



#1. External Network Interface

#2. Method of Desktop Refresh

MAG-TA Concept



The Enterprise View

NMCI
NAVY MARINE CORPS INTRANET